Guia do administrador

Amazon Nimble Studio

Amazon Nimble Studio: Guia do administrador

Table of Contents

O que é o Amazon Nimble Studio?

O Nimble Studio fornece infraestrutura e gerenciamento centralizado para um conjunto de aplicações e serviços que os artistas podem usar para produzir efeitos visuais, animação e conteúdo de jogos na nuvem.

Com o Nimble Studio, você obtém ferramentas essenciais para gerenciamento de usuários e grupos. Você também pode adicionar e gerenciar aplicações, incluindo AWS, Thinkbox e o Nimble Studio File Transfer.

O Nimble Studio apresenta uma interface unificada que coloca todos os atributos do seu estúdio em um só lugar. Você pode integrar usuários, atribuir aplicações e anexar permissões específicas para suas funções de trabalho. O Nimble Studio não requer experiência AWS e você pode configurá-lo em cerca de cinco minutos.

Índice

Atributos e benefícios

Aqui estão alguns dos atributos e benefícios que você obtém com o Nimble Studio:

- Use o Nimble Studio gratuitamente; pague somente pelos recursos de estúdio que suas aplicações usam.
- Gerencie centralmente seu estúdio, verifique seu status e obtenha informações de alto nível sobre sua operação.
- Adicione e gerencie aplicações, usuários e grupos do Nimble Studio e anexe permissões.
- Gerencie com segurança o acesso aos recursos do estúdio com políticas e perfis AWS Identity and Access Management (IAM).
- Gerencie a segurança de login para usuários do estúdio e provedores de identidade externos com AWS IAM Identity Center (IAM Identity Center).
- Organize e encontre facilmente os recursos do estúdio com tags nos recursos do seu estúdio.

Aplicações relacionadas

O Nimble Studio fornece aplicações para criadores de conteúdo digital operarem um estúdio baseado em nuvem para produzir efeitos visuais (VFX), animação e conteúdo interativo.

Você pode instalar esses aplicações no seu computador local ou na nuvem com uma instância do Amazon Elastic Compute Cloud (Amazon EC2). Você pode também usar o Amazon Simple Storage Service (Amazon S3) para transferir e armazenar ativos de mídia digital de forma segura. Isso significa que você pode usar o Nimble Studio para reduzir os custos de infraestrutura física, equipamentos e equipe técnica.

Atualmente, o Nimble Studio fornece os seguintes aplicações:

- AWS Thinkbox: o Thinkbox software inclui o gerente do parque de renderização Deadline Thinkbox e o plugin 3D, Krakatoa Thinkbox. Você pode usar o software Thinkbox para ajudá-lo a aumentar a produção criativa do seu estúdio on-premises, na nuvem com o Amazon EC2 ou uma combinação de ambos. Para obter mais informações, consulte ProdutosAWS Thinkbox.
- Nimble Studio File Transfer: File Transfer acelera as transferências de ativos de mídia digital de e para o Amazon S3. File Transfer fornece uma interface gráfica de usuário, que você pode usar para mover rapidamente milhares de arquivos de mídia grandes. Para obter mais informações, consulte a página O que éNimble Studio File Transfer.

Preços do Nimble Studio

Não há cobrança para configurar o Nimble Studio e usá-lo para gerenciar a infraestrutura, os usuários, a segurança e os serviços do seu estúdio.

No entanto, se você configurar serviços e aplicações em seu estúdio, poderá ser cobrado pelo armazenamento e outros recursos do estúdio. Para obter mais informações sobre a definição de preço da aplicação Nimble Studio, consulte a página de preço da aplicação individual.

Para obter informações sobre como gerenciar seus custos AWS, consulte AWS Cost Explorer Service e AWS Budgets.

Comece a usar o Nimble Studio

A configuração e implantação do Nimble Studio levam cerca de cinco minutos.

Depois de se familiarizar com os conceitos e a terminologia do Nimble Studio, consulte Introdução ao Amazon Nimble Studio. Nele, você encontrará instruções passo a passo para implantar o estúdio.

Conceitos e terminologia do Amazon Nimble Studio

Para ajudar você a começar a usar o Amazon Nimble Studio e entender como ele funciona, consulte os principais conceitos e terminologia deste guia.

Recursos principais

Amazon Nimble Studio

O Amazon Nimble Studio é um AWS service (Serviço da AWS) que permite que estúdios criativos produzam efeitos visuais, animação e conteúdo interativo inteiramente na nuvem, desde o esboço do storyboard até a entrega final.

Amazon Nimble Studio

O console do Nimble Studio é uma parte do AWS Management Console que é dedicado aos nossos clientes administrativos de TI. Esse console é onde os administradores criam seu estúdio na nuvem e gerenciam várias configurações. Por exemplo, a página do gerenciador do Studio permite que você adicione ou remova recursos, adicione aplicações e conceda permissões a usuários e grupos.

Amazon Nimble Studio

O portal do Nimble Studio fornece uma interface de usuário para interações diárias com as aplicações e serviços do Nimble Studio. Os usuários entram diretamente no portal com seu nome de usuário e senha sem precisar interagir com AWS Management Console.

Nimble Studio File Transfer

File Transfer acelera as transferências de ativos de mídia de ativos de mídia digital de e para o Amazon Simple Storage Service (Amazon S3). File Transfer fornece uma interface gráfica de usuário, que você pode usar para mover rapidamente milhares de arquivos de mídia grandes. Para obter mais informações, consulte a página O que é?.

AWS Thinkbox

O software Thinkbox inclui o parque de renderização, o Deadline Thinkbox e o plugin 3D, Krakatoa Thinkbox. Você pode usar o software Thinkbox para ajudá-lo a aumentar a produção criativa do seu estúdio on-premises, na nuvem com o Amazon EC2 ou uma combinação de ambos. Para obter mais informações, consulte Produtos AWS Thinkbox.

Conceitos principais e terminologia

Políticas gerenciadas por AWS

Uma AWS política gerenciada pela é uma política independente que é criada e administrada pela AWS. Política independente significa que a política tem seu próprio nome de recurso da Amazon (ARN) que inclui o nome da política. Por exemplo, arn:aws:iam::aws:policy/IAMReadOnlyAccess é uma política gerenciada por AWS. Para obter mais informações sobre ARNs, consulte ARNs do IAM.

Políticas gerenciadas por AWS são usadas para conceder permissões para funções de trabalho comuns. As políticas de função de trabalho são mantidas e atualizadas quando AWS novos serviços e operações de API são introduzidos. Por exemplo, a função de trabalho AdministratorAccess fornece acesso total e delegação de permissões para cada serviço e recurso na AWS. Por outro lado, políticas gerenciadas por AWS de acesso parcial, como AmazonMobileAnalyticsWriteOnlyAccess e AmazonEC2ReadOnlyAccess, podem fornecer níveis específicos de acesso a Serviços da AWS sem permitir o acesso total. Para obter mais informações sobre políticas de acesso, consulte Noções básicas sobre resumos de nível de acesso em resumos de política.

AWS Management Console

O AWS Management Console é uma aplicação da web que fornece acesso a uma ampla coleção de consoles de serviço para gerenciamento de aplicações Serviços da AWS.

Cada serviço também inclui seu próprio console. Esses consoles oferecem uma ampla variedade de ferramentas para computação em nuvem. Existe até um serviço que ajuda no faturamento e no gerenciamento de custos.

IAM Identity Center AWS IAM Identity Center

O IAM Identity Center é um serviço AWS que facilita o gerenciamento centralizado do acesso a várias aplicações Contas da AWS comerciais. Com o IAM Identity Center, você poderá fornecer aos usuários acesso de logon único a todas as contas e aplicações atribuídas em um só lugar. Você também pode gerenciar centralmente o acesso a várias contas e as permissões de usuário para todas as suas contas no AWS Organizations. Para obter mais informações, visite Perguntas frequentes AWS IAM Identity Center.

AWSPrivateLink

O PrivateLink AWS fornece conectividade privada entre VPCs, Serviços da AWS e suas redes on-premises, sem expor seu tráfego à Internet pública. AWS PrivateLink facilita a conexão de serviços

em diferentes contas e VPCs. AWS PrivateLink está disponível por uma taxa mensal que é cobrada de você Conta da AWS.

Criação de conteúdo digital (DCC)

Criação de conteúdo digital (DCC) se refere à categoria de aplicações usadas para produzir conteúdo criativo, incluindo Blender, Nuke, Maya e Houdini.

Regiões

O Nimble Studio oferece onze opções Regiões da AWS para você escolher e implantar seu estúdio. As regiões são onde existe a infraestrutura essencial do estúdio, como seus dados e aplicações.

A região deve estar localizada mais próxima dos usuários do seu estúdio. Isso reduz o atraso e melhora as velocidades de transferência de dados.

Studio

Um estúdio é o contêiner de nível superior para outros recursos relacionados ao Nimble Studio. Seu estúdio em nuvem gerencia o portal web do Nimble Studio e as conexões com recursos essenciais em seu Conta da AWS, como sua VPC, diretório de usuários e chaves de criptografia de armazenamento.

Aplicações do Studio

Os componentes do Studio são configurações no Nimble Studio de um cliente que informam ao serviço como acessar recursos como sistemas de arquivos, servidores de licenças e parques de renderização em seu Conta da AWS.

O Nimble Studio contém vários subtipos de componentes de estúdio, incluindo um sistema de arquivos compartilhado, fazenda de computação, Active Directory e componente de licença. Esses subtipos descrevem os recursos que você gostaria que seu estúdio usasse.

Recursos do Studio

Recursos do Studio é um termo que encapsula as coisas que um estúdio precisa em suas operações diárias. Ao descrever como os recursos se encaixam na infraestrutura de um estúdio em nuvem, eles também podem ser chamados de componentes de estúdio.

Tags

Uma tag é um rótulo atribuído a um recurso da AWS. Cada tag consiste em uma chave e um valor opcional que você define.

As etiquetas permitem categorizar seus recursos da AWS de maneiras diferentes. Por exemplo, você pode definir um conjunto de tags para as instâncias do Amazon Elastic Compute Cloud (Amazon EC2) da sua conta que ajudam a rastrear o proprietário e o nível de pilha de cada instância. As tags também permitem que você integre os sistemas de arquivos compartilhados e os parques de renderização de sua organização com o Nimble Studio, para manter seus fluxos de trabalho ininterruptos enquanto você move sua força de trabalho para a nuvem.

Com tags, você pode categorizar seus recursos AWS por finalidade, proprietário ou ambiente. Isso é útil quando você tem muitos recursos do mesmo tipo — é possível identificar rapidamente um recurso específico baseado nas tags que você atribuiu a ele.

Configurar o Nimble Studio

Este tutorial é para usuários administradores que desejam configurar um Amazon Nimble Studio.

As seções a seguir guiarão você pelas etapas que precisa concluir antes de implantar um estúdio no Nimble Studio.

Conteúdo

Configurar IAM

Analise o seguinte AWS Identity and Access Management (IAM) documentação antes de começar.

- Práticas recomendadas de segurança no IAM
- Faça login no seu Conta da AWS como usuário administrador para concluir a configuração restante.

Inscreva-se para um Conta da AWS

Se você não tiver um Conta da AWS, conclua as etapas a seguir para criar uma.

Para se inscrever em um Conta da AWS

1. Abra a https://portal.aws.amazon.com/billing/inscrição.
2. Siga as instruções online.

   Parte do procedimento de inscrição envolve receber uma chamada telefônica e inserir um código de verificação no teclado do telefone.

   Quando você se inscreve em um Conta da AWS, um Usuário raiz da conta da AWSé criado. O usuário root tem acesso a todos Serviços da AWS e recursos na conta. Como prática recomendada de segurança, atribua o acesso administrativo a um usuário e use somente o usuário-raiz para executar tarefas que exigem acesso de usuário-raiz.

AWS envia um e-mail de confirmação após a conclusão do processo de inscrição. A qualquer momento, você pode visualizar a atividade atual da sua conta e gerenciar sua conta acessando https://aws.amazon.com/e escolhendo Minha conta.

Criar um usuário com acesso administrativo

Depois de se inscrever em um Conta da AWS, proteja seu Usuário raiz da conta da AWS, habilitar AWS IAM Identity Center e crie um usuário administrativo para que você não use o usuário root nas tarefas diárias.

Proteja seu Usuário raiz da conta da AWS

1. Faça login no AWS Management Consolecomo proprietário da conta, escolhendo o usuário root e inserindo seu Conta da AWS endereço de e-mail. Na próxima página, insira sua senha.

   Para obter ajuda para fazer login usando o usuário root, consulte Como fazer login como usuário root no Início de Sessão da AWS Guia do usuário.
2. Ative a autenticação multifator (MFA) para seu usuário root.

   Para obter instruções, consulte Habilitar um MFA dispositivo virtual para seu Conta da AWS usuário root (console) no Guia do IAM usuário.

Criar um usuário com acesso administrativo

1. Ative o IAM Identity Center.

   Para obter instruções, consulte Habilitando AWS IAM Identity Center no AWS IAM Identity Center Guia do usuário.
2. No IAM Identity Center, conceda acesso administrativo a um usuário.

   Para um tutorial sobre como usar o Diretório do Centro de Identidade do IAM como sua fonte de identidade, consulte Configurar o acesso do usuário com o padrão Diretório do Centro de Identidade do IAM no AWS IAM Identity Center Guia do usuário.

Iniciar sessão como o usuário com acesso administrativo

- Para entrar com seu usuário do IAM Identity Center, use o login URL que foi enviado ao seu endereço de e-mail quando você criou o usuário do IAM Identity Center.

Para obter ajuda para fazer login usando um usuário do IAM Identity Center, consulte Como fazer login no AWS portal de acesso no Início de Sessão da AWS Guia do usuário.

Atribuir acesso a usuários adicionais

1. No IAM Identity Center, crie um conjunto de permissões que siga as melhores práticas de aplicação de permissões com privilégios mínimos.

   Para obter instruções, consulte Criar um conjunto de permissões no AWS IAM Identity Center Guia do usuário.
2. Atribua usuários a um grupo e, em seguida, atribua o acesso de autenticação única ao grupo.

   Para obter instruções, consulte Adicionar grupos no AWS IAM Identity Center Guia do usuário.

Recursos relacionados

- Práticas recomendadas de segurança no IAM
- AWS service (Serviço da AWS) cotas - Referência geral da AWS

Conceitos básicos do Amazon Nimble Studio

Este capítulo mostra como usar o console do Nimble Studio para criar a infraestrutura do seu estúdio, confirmar Região da AWS, revisar as configurações e criar seu estúdio. Você também pode personalizar sua configuração com configurações adicionais.

Para clientes iniciantes AWS, consulte os tutoriais Configurar o Nimble Studio.

Tópicos

Configurar o Nimble Studio

Este guia mostra como configurar sua infraestrutura, revisar suas configurações e criar seu estúdio. Você também pode personalizar seu estúdio com Configurações adicionais do Studio.

Etapa 1: configurar o Studio Infrastructure

A infraestrutura do seu estúdio consiste nos componentes a seguir:

- Nome de exibição do estúdio: O nome de exibição do Studio é como você pode identificar seu estúdio — por exemplo, AnyCompanyStudio. O nome do seu estúdio também determina a URL do portal do Studio. Você pode alterar o nome de exibição do Studio depois de concluir a configuração, a qualquer momento.
- URL do portal do Studio: você pode acessar seu estúdio usando a URL do portal do Studio. O URL é baseado no nome de exibição do Studio — por exemplo, https://anycompanystudio.awsapps.com. Você pode alterar a URL do portal do Studio depois de concluir a configuração, a qualquer momento.
- Região da AWS: Região da AWS é o local físico de uma coleção de data centers AWS. Quando você configura seu estúdio, o padrão da Região é o local mais próximo de você Você deve alterar a região para que ela fique mais próxima de seus usuários. Isso reduz o atraso e melhora as velocidades de transferência de dados.

> **Important**
>
> Você não pode mudar sua região depois de terminar de configurar o Nimble Studio.

Conclua as tarefas nesta seção para configurar a infraestrutura do seu estúdio.

Para configurar a infraestrutura do seu estúdio

1. Faça login em AWS Management Console e abra o console do Nimble Studio.
2. Escolha Configurar o Nimble Studio e, em seguida, escolha Avançar.
3. Insira o nome de exibição do Studio — por exemplo **`AnyCompany Studio`**.
4. (Opcional) Para alterar o nome do portal do Studio, escolha Editar URL.
5. (Opcional) Para alterar para Região da AWSque fique mais próximo dos usuários do seu estúdio, escolha Alterar região.
   a. Escolha a região mais próxima para a maioria dos seus usuários.
   b. Escolha Aplicar região.
6. (Opcional) Para personalizar ainda mais a configuração do seu estúdio, selecione Configurações adicionais do Studio.
7. Para revisar suas configurações antes de criar seu estúdio, escolha Avançar.

Etapa 2: revisar e criar o seu estúdio

Depois de configurar a infraestrutura do seu estúdio, você pode revisar, fazer alterações e criar seu estúdio.

Para revisar e criar seu estúdio

1. Na página Revisar e criar, revise sua infraestrutura do Studio.
2. Confirme se o Região da AWS é o mais próximo dos usuários do seu estúdio.
3. (Opcional) Escolha Editar para fazer alterações na configuração do seu estúdio.
4. Quando quiser, escolha Criar estúdio.

Configurações adicionais do Studio

A configuração do Nimble Studio inclui configurações adicionais de estúdio. Com essas configurações, você pode visualizar todas as alterações que a configuração do Nimble Studio faz em seu Conta da AWS, configurar sua função de usuário do estúdio e alterar o tipo de chave de criptografia. Você também pode adicionar tags opcionais aos recursos do estúdio.

Configurar a função de usuário do estúdio

Um serviço AWS pode assumir uma função de serviço para executar ações em seu nome. O Nimble Studio requer um perfil de usuário de estúdio para dar aos usuários acesso aos recursos em seu estúdio.

Você pode anexar políticas gerenciadas AWS Identity and Access Management (IAM) ao perfil de usuário do estúdio. As políticas permitem que os usuários realizem determinadas ações, como criar trabalhos em uma aplicação específica do Nimble Studio. Como as aplicações dependem de condições específicas na política gerenciada, se você não usar as políticas gerenciadas, a aplicação pode não funcionar conforme o esperado.

Você pode alterar o perfil do usuário do Studio depois de concluir a configuração, a qualquer momento. Para obter mais informações sobre perfis de usuário, consulte Perfis do IAM.

As guias a seguir contêm instruções para dois casos de uso diferentes. Para criar e usar um novo perfil de serviço, escolha a guia Novo perfil de serviço. Para usar um perfil de serviço existente, escolha a guia Perfil de serviço existente.

New service role

Para criar e usar um novo perfil de serviço

1. Selecione Criar e usar um novo perfil de serviço.
2. (Opcional) Insira um nome de perfil de usuário do serviço.
3. Escolha Exibir detalhes da permissão para obter mais informações sobre a função.

Existing service role

Para usar um perfil de serviço existente

1. Selecione Usar um perfil de serviço existente.

2. Abra a lista suspensa para escolher um perfil de serviço existente.
3. (Opcional) Escolha Exibir no console do IAM para obter mais informações sobre o perfil.

AWS IAM Identity Center

AWS IAM Identity Center é um serviço de login único baseado em nuvem para gerenciar usuários e grupos. O IAM Identity Center também pode ser integrado ao seu provedor corporativo de autenticação única (SSO) para que os usuários possam fazer login com a conta da empresa.

O Nimble Studio habilita o IAM Identity Center por padrão e é necessário configurar e usar o Nimble Studio. Para obter mais informações, consulte O que é o AWS IAM Identity Center.

Configurar chave de criptografia AWS KMS

As chaves AWS Key Management Service (AWS KMS) são o principal tipo de chave do KMS que você pode usar para criptografar, descriptografar e recriptografar dados.

O Nimble Studio inclui os seguintes tipos de chave AWS KMS de criptografia:

- Chave de propriedade AWS – AWS chaves de propriedade são chaves KMS que AWS service (Serviço da AWS) ela possui e gerencia para uso em vários arquivos Contas da AWS. As chaves próprias AWS não residem em sua conta Conta da AWS, mas o Nimble Studio pode usar uma chave própria AWS para proteger os recursos em sua conta.

  Para usar AWS KMS, você não precisa criar ou manter a chave ou sua política de chaves. Não há cobrança pelo uso de chaves próprias AWS e elas não contam nas cotas AWS KMS de sua propriedade Conta da AWS.
- Chave gerenciada pelo cliente AWS KMS – Uma chave gerenciada pelo cliente é uma chave do KMS na sua Conta da AWS criada e gerenciada por você.

  Você tem controle total sobre essas chaves KMS. As chaves gerenciadas pelo cliente incorrem em uma taxa mensal. Eles também cobram uma taxa para cada solicitação de API AWS KMS além do nível gratuito. Para obter mais informações sobre definição de preço do AWS KMS, consulte Definição de preço do AWS Key Management Service.

O tipo de chave de criptografia não pode ser alterado após a conclusão da configuração. Para obter mais informações AWS KMS e tipos de chaves de criptografia, consulte a documentação AWS KMS.

Para escolher um tipo de chave de criptografia diferente

1. Selecione Escolher uma tecla diferente AWS KMS (avançada).
2. Selecione uma chave AWS KMS ou insira um número de recurso da Amazon (ARN).
3. Escolha Criar chave AWS KMS.

Configurar tags

As tags funcionam como etiquetas para organizar seus recursos do Nimble Studio. Você pode adicionar até 50 tags para identificar, organizar, filtrar e pesquisar recursos.

Cada tag consiste em duas partes, que você define: uma chave de tag e um valor de tag opcional – por exemplo, chave: `domain` e valor: `anycompanystudio.com`.

Você pode adicionar ou remover tags após concluir a configuração a qualquer momento. Para obter mais informações sobre tags, consulte Marcando seus recursos AWS.

Para adicionar tags aos recursos do seu estúdio

1. Selecione Add new tag (Adicionar nova tag).
2. Insira a tag Key (Chave).
3. (Opcional) Insira o Valor da tag.

Excluir um estúdio

Se você não precisa mais do estúdio, você pode excluí-lo. Quando você exclui seu estúdio, somente a infraestrutura do estúdio é excluída. Seus outros recursos AWS, como perfis de usuário, políticas e dados de aplicações, permanecem intactos.

> **Important**
>
> Não é possível recuperar um estúdio após sua exclusão.

Para excluir seu estúdio

1. Faça login em AWS Management Console e abra o console do Nimble Studio.
2. Selecione Visão geral do Studio.
3. Selecione Ações e escolha Excluir estúdio.
4. Insira **`delete`** e escolha Excluir.

Segurança em Amazon Nimble Studio

Segurança na nuvem em AWS é a maior prioridade. Como um AWS cliente, você se beneficia de data centers e arquiteturas de rede criados para atender aos requisitos das organizações mais sensíveis à segurança.

A segurança é uma responsabilidade compartilhada entre AWS e você. O modelo de responsabilidade compartilhada descreve isso como segurança da nuvem e segurança na nuvem:

- Segurança da nuvem — AWS é responsável por proteger a infraestrutura que funciona AWS serviços no Nuvem AWS. AWS também fornece serviços que você pode usar com segurança. Auditores terceirizados testam e verificam regularmente a eficácia de nossa segurança como parte do AWS Programas de conformidade . Para saber mais sobre os programas de conformidade que se aplicam ao Amazon Nimble Studio, veja AWS Serviços no escopo do Programa de Conformidade .
- Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você usa. Você também é responsável por outros fatores, incluindo a confidencialidade de seus dados, os requisitos da empresa e as leis e regulamentos aplicáveis.

> **Important**
>
> É altamente recomendável que você leia e se familiarize com o Pilar de Segurança - AWS Well-Architected Framework. Este artigo contém os principais princípios para proteger seu AWS infraestrutura.

Esta documentação ajuda você a entender como aplicar o modelo de responsabilidade compartilhada ao usar Nimble Studio. Os tópicos a seguir mostram como configurar Nimble Studio para atender aos seus objetivos de segurança e conformidade. Você também aprende a usar outros AWS serviços que ajudam você a monitorar e proteger seu Nimble Studio recursos.

Mais informações

- Pilar de segurança - AWS Estrutura Well-Architected
- Segurança para o AWS Cloud Development Kit (AWS CDK) (AWS CDK)
- Segurança na Amazon Virtual Private Cloud (VPC)

- AWS credenciais de segurança
- Segurança na Amazon EC2
  - Linux
  - Windows

Configurar Conta da AWS segurança

Este guia mostra como configurar seu Conta da AWS para receber notificações quando seus recursos estão comprometidos e para permitir notificações específicas Conta da AWS usuários para acessá-lo. Para proteger seu Conta da AWS e acompanhe seus recursos, conclua as etapas a seguir.

Conteúdo

- Exclua as chaves de acesso da sua conta
- Habilitar a autenticação multifator
- Habilitar CloudTrail em todos Regiões da AWS
- Configure a Amazon GuardDuty e as notificações

Exclua as chaves de acesso da sua conta

Você pode permitir o acesso programático ao seu AWS recursos do AWS Command Line Interface (AWS CLI) ou com AWS APIs. No entanto, AWS recomenda que você não crie nem use as chaves de acesso associadas à sua conta raiz para acesso programático.

Se você ainda tiver chaves de acesso, recomendamos excluí-las e criar um usuário. Em seguida, conceda a esse usuário somente as permissões necessárias para o APIs que você planeja ligar. Você pode usar esse usuário para emitir chaves de acesso.

Para obter mais informações, consulte Gerenciando chaves de acesso para seu Conta da AWS no Referência geral da AWS guia.

Habilitar a autenticação multifator

A autenticação multifator (MFA) é um recurso de segurança que fornece uma camada de autenticação além do seu nome de usuário e senha.

MFAfunciona assim: depois de fazer login com seu nome de usuário e senha, você também deve fornecer uma informação adicional à qual somente você tenha acesso físico. Essas informações podem vir de um dispositivo MFA de hardware dedicado ou de um aplicativo em um telefone.

Você deve selecionar o tipo de MFA dispositivo que deseja usar na lista de MFA dispositivos compatíveis. Para um dispositivo de hardware, mantenha o MFA dispositivo em um local seguro.

Se você usa um MFA dispositivo virtual (como um aplicativo de telefone), pense no que pode acontecer se o telefone for perdido ou danificado. Uma abordagem é manter o MFA dispositivo virtual que você usa em um local seguro. Outra opção é ativar mais de um dispositivo ao mesmo tempo ou usar uma MFA opção virtual para recuperar a chave do dispositivo.

Para saber maisMFA, consulte Habilitando um dispositivo de autenticação multifator virtual (MFA).

Recursos relacionados

- Conceitos básicos da autenticação multifatorial
- Protegendo o acesso a AWS Usando MFA

Habilitar CloudTrail em todos Regiões da AWS

Você pode acompanhar todas as atividades em seu AWS recursos usando AWS CloudTrail. Recomendamos que você ative CloudTrail agora. Isso pode ajudar AWS Support e seu AWS o arquiteto de soluções soluciona um problema de segurança ou configuração posteriormente.

Para habilitar o CloudTrail login em todos Regiões da AWS, veja AWS CloudTrail Atualização — Ative em todas as regiões e use várias trilhas.

Para saber mais sobre CloudTrail, consulte Ativar CloudTrail: registrar API atividades em seu Conta da AWS. Para saber como CloudTrail monitora o Nimble Studio, consulteRegistrando chamadas do Nimble Studio usando AWS CloudTrail.

Configure a Amazon GuardDuty e as notificações

A Amazon GuardDuty é um serviço contínuo de monitoramento de segurança que analisa e processa o seguinte:

- Fontes de dados
- Registros VPC de fluxo da Amazon

- AWS CloudTrail registros de eventos de gerenciamento
- CloudTrail Registros de eventos de dados do S3
- DNStroncos

A Amazon GuardDuty identifica atividades inesperadas, potencialmente não autorizadas e maliciosas em seu AWS meio ambiente. A atividade maliciosa pode incluir problemas como escalonamento de privilégios, uso de credenciais expostas ou comunicação com endereços IP ou domínios maliciosos. Para identificar essas atividades, GuardDuty usa feeds de inteligência de ameaças, como listas de endereços IP e domínios maliciosos e aprendizado de máquina. Por exemplo, GuardDuty pode detectar EC2 instâncias comprometidas da Amazon servindo malware ou minerando bitcoins.

GuardDuty também monitora Conta da AWS comportamento de acesso em busca de sinais de comprometimento. Isso inclui implantações de infraestrutura não autorizadas, como instâncias implantadas em um Região da AWS que nunca foi usado. Também inclui API chamadas incomuns, como uma alteração na política de senha para reduzir a força da senha.

GuardDuty informa você sobre o status do seu AWS ambiente por meio da produção de descobertas de segurança. Você pode ver essas descobertas no GuardDuty console ou por meio de CloudWatch eventos da Amazon.

Configurar um SNS tópico e um endpoint da Amazon

Siga as instruções no tutorial Configurar um SNS tópico e endpoint da Amazon.

Configure um EventBridge evento para GuardDuty descobertas

Crie uma regra EventBridge para enviar eventos para todas as descobertas GuardDuty geradas.

Para criar um EventBridge evento para GuardDuty descobertas

1. Faça login no EventBridge console da Amazon: https://console.aws.amazon.com/events/
2. No painel de navegação, escolha Regras. Em seguida, escolha Create rule (Criar regra).
3. Insira um Nome e uma Descrição para a nova regra. Em seguida, escolha Próximo.
4. Sair AWS eventos ou eventos de EventBridge parceiros selecionados para a fonte do evento.
5. Em Padrão de evento, escolha AWS serviços para a fonte do evento. Então, GuardDutypara o AWS serviços e GuardDuty Busca para o tipo de evento. Este é o tópico que você criou em Configurar um SNS tópico e um endpoint da Amazon.
6. Escolha Próximo.

7. Para o Target 1, selecione AWS serviço. Escolha o SNStópico no menu suspenso Selecionar um destino. Em seguida, escolha seu GuardDutytópico _to_email.
8. Na seção Configurações adicionais: Use o menu suspenso Configurar entrada de destino para escolher Transformador de entrada. Selecione Configurar transformador de entrada.
9. Insira o código a seguir no campo Caminho de entrada na seção Transformador de entrada de destino.

```
{
    "severity": "$.detail.severity",
    "Account_ID": "$.detail.accountId",
    "Finding_ID": "$.detail.id",
    "Finding_Type": "$.detail.type",
    "region": "$.region",
    "Finding_description": "$.detail.description"
}
```

10. Para formatar o e-mail, insira o código a seguir no campo Modelo.

```
"AWS <Account_ID> has a severity <severity> GuardDuty finding type <Finding_Type>
 in the <region> region."
"Finding Description:"
"<Finding_description>. "
"For more details open the GuardDuty console at https://console.aws.amazon.com/
guardduty/home?region=<region>#/findings?search=id=<Finding_ID>"
```

11. Escolha Criar. Em seguida, escolha Próximo.
12. (Opcional) Adicione tags se você estiver usando tags para rastrear suas AWS recursos.
13. Escolha Próximo.
14. Revise sua regra. Em seguida, escolha Create rule (Criar regra).

Agora que você configurou seu Conta da AWS segurança, você pode conceder acesso a usuários específicos e receber notificações quando seus recursos forem comprometidos.

Proteção de dados em Amazon Nimble Studio

A ferramenta AWS modelo de responsabilidade compartilhada modelo se aplica à proteção de dados em Amazon Nimble Studio. Conforme descrito neste modelo, AWS é responsável por proteger a infraestrutura global que executa todas as Nuvem AWS. Você é responsável por manter o controle

sobre o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança do Serviços da AWS que você usa. Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na Europa, consulte AWS Modelo de responsabilidade compartilhada e postagem no GDPR blog sobre o AWS Blog de segurança.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS recursos. Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Configure API e registre as atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Trabalhando com CloudTrail trilhas no AWS CloudTrail Guia do usuário.
- Use AWS soluções de criptografia, junto com todos os controles de segurança padrão dentro Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de FIPS 140-3 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um FIPS endpoint. Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-3.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de e-mail dos seus clientes, em marcações ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com Nimble Studio ou outro Serviços da AWS usando o consoleAPI, AWS CLI, ou AWS SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, é altamente recomendável que você não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

A ferramenta AWS O modelo de responsabilidade compartilhada se aplica à proteção de dados no Amazon Nimble Studio. Conforme descrito neste modelo, AWS é responsável por proteger a

infraestrutura global que executa todas as Nuvem AWS. Você é responsável por manter o controle sobre o conteúdo hospedado nessa infraestrutura. Esse conteúdo inclui as tarefas de configuração e gerenciamento de segurança do Serviços da AWS que você usa.

Para obter mais informações sobre privacidade de dados, consulte Privacidade de dados FAQ. Para obter informações sobre proteção de dados na União Europeia, visite o GDPRCentro.

Criptografia em repouso

O Nimble Studio protege dados confidenciais do estúdio criptografando-os em repouso usando chaves de criptografia armazenadas em AWS Key Management Service (AWS KMS). A criptografia em repouso está disponível em todos Regiões da AWS onde o Nimble Studio está disponível. Os dados de estúdio que criptografamos incluem o nome e as descrições de todos os tipos de recursos, bem como scripts de componentes de estúdio, parâmetros de script, pontos de montagem, nomes de compartilhamento e outros dados.

Criptografar dados significa que dados confidenciais salvos em discos não podem ser lidos por nenhum usuário ou aplicativo sem uma chave válida. Os dados criptografados podem ser armazenados com segurança em repouso e podem ser descriptografados somente por uma parte com acesso autorizado à chave gerenciada.

Para obter informações sobre como o Nimble Studio usa AWS KMS para criptografar dados em repouso, consulteGerenciamento de chaves do Amazon Nimble Studio.

Usando subsídios com AWS KMS keys

Um subsídio é um instrumento político que permite AWS princípios a serem usados AWS KMS chaves em operações criptográficas. Também permite que eles visualizem uma KMS chave com o comando `DescribeKey` e criem e gerenciem concessões.

Os subsídios são comumente usados por Serviços da AWS que se integram com AWS KMS para criptografar seus dados em repouso. O serviço cria uma concessão em nome de um usuário na conta, usa suas permissões e desativa a concessão assim que sua tarefa é concluída.

Quando o Nimble Studio cria seu estúdio, fornecemos duas funções para os usuários do portal do Nimble Studio: funções de usuário e administrador. O Nimble Studio cria concessões em chaves gerenciadas pelo cliente para esses perfis a fim de fornecer acesso aos dados criptografados do estúdio.

> **Important**
>
> Se você excluir uma concessão, o portal do Nimble Studio ficará inutilizável para os usuários até que o administrador crie uma nova concessão.

Para obter detalhes sobre como Serviços da AWS use subsídios, veja Como Serviços da AWS use AWS KMS ou o tópico Criptografia em repouso no guia do usuário ou no guia do desenvolvedor do serviço.

Criptografia em trânsito

A tabela a seguir fornece informações sobre como os dados são criptografados em trânsito. Quando aplicável, outros métodos de proteção de dados do Nimble Studio também são listados.

Dados	Caminho de rede	Proteção
Ativos da Web, como imagens e JavaScript arquivos	O caminho da rede é entre os usuários do Nimble Studio e o Nimble Studio.	A criptografia de dados usa TLS 1.2 ou posterior.
Tráfego de pixel e streaming relacionado	O caminho da rede é entre os usuários do Nimble Studio e o Nimble Studio.	Criptografado usando o Advanced Encryptio n Standard de 256 bits (AES-256) e transportado usando TLS 1.2 ou posterior.
APItráfego	O caminho é entre os usuários do Nimble Studio e o Nimble Studio.	Criptografado usando TLS 1.2 ou posterior. As solicitações para criar uma conexão são assinadas usando SigV4.

Gerenciamento de chaves do Amazon Nimble Studio

Ao criar um novo estúdio, você pode escolher uma das seguintes chaves para criptografar os dados do seu estúdio:

- AWS KMSchave própria — Tipo de criptografia padrão. A chave é propriedade do Nimble Studio (sem custo adicional).
- KMSChave gerenciada pelo cliente — A chave é armazenada em sua conta e é criada, de propriedade e gerenciada por você. Você tem controle total sobre a chave. AWS KMS cobranças se aplicam.

Excluindo uma KMS chave gerenciada pelo cliente em AWS Key Management Service (AWS KMS) é destrutivo e potencialmente perigoso. Exclui irreversivelmente o material da chave e todos os metadados associados à chave. Depois que uma KMS chave gerenciada pelo cliente é excluída, você não pode mais descriptografar os dados que foram criptografados por essa chave. Isso significa que os dados se tornam irrecuperáveis.

É por isso AWS KMS oferece aos clientes um período de espera de até 30 dias antes de excluir a chave. O período de espera padrão é de 30 dias.

Sobre o período de espera

Como é destrutivo e potencialmente perigoso excluir uma KMS chave gerenciada pelo cliente, exigimos que você defina um período de espera de 7 a 30 dias. O período de espera padrão é de 30 dias.

No entanto, o período de espera real pode ser até 24 horas mais longo do que o programado. Para obter a data e a hora reais em que a chave será excluída, use a DescribeKeyoperação. Você também pode ver a data de exclusão programada de uma chave no AWS KMS console na página de detalhes da chave, na seção Configuração geral. Observe o fuso horário.

Durante o período de espera, o status e o estado da chave gerenciada pelo cliente são Exclusão pendente.

- Uma KMS chave gerenciada pelo cliente que está pendente de exclusão não pode ser usada em nenhuma operação criptográfica.
- AWS KMS não gira as chaves de apoio do cliente gerenciado AWS KMS chaves que estão pendentes de exclusão.

Para obter mais informações sobre como excluir um cliente gerenciado AWS KMS chave, consulte Excluindo chaves mestras do cliente.

Medidas de segurança dos dados

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS credenciais e configure contas individuais com AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.
- UseSSL/TLSpara se comunicar com AWS recursos. Recomendamos TLS 1.2 ou posterior.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use AWS soluções de criptografia, junto com todos os controles de segurança padrão dentro Serviços da AWS.
- Se você precisar de FIPS 140-2 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um FIPS endpoint. Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de contas de clientes, em campos de formato livre, como o campo Nome. Isso inclui quando você trabalha com o Amazon Nimble Studio ou outro Serviços da AWS usando o consoleAPI, AWS CLI, ou AWS SDKs. Todos os dados inseridos no Amazon Nimble Studio ou em outros serviços podem ser coletados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Dados e métricas de diagnóstico

Durante a implantação e exclusão do StudioBuilder, o Amazon Nimble Studio coleta determinadas métricas que usamos para diagnosticar problemas e melhorar os recursos e a experiência do usuário do Nimble Studio.

Tipos de métricas coletadas

- Informações de uso — Os comandos e subcomandos genéricos que são executados.
- Erros e informações de diagnóstico — O status e a duração dos comandos que são executados, incluindo códigos de saída, nomes de exceções internas e falhas.

- Informações do sistema e do ambiente — A versão do Python, sistema operacional (Windows, Linux, ou macOS) e o ambiente em que StudioBuilder é executado.

Gerenciamento de identidade e acesso para Amazon Nimble Studio

AWS Identity and Access Management (IAM) é um AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso ao AWS recursos. Os administradores controlam quem pode ser autenticado (conectado) e autorizado (ter permissões) para usar os recursos do Amazon Nimble Studio. IAMé um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

Como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz no Nimble Studio.

Usuário do serviço: se você usar o serviço Nimble Studio para fazer o trabalho, é um usuário do serviço. Nesse caso, o administrador fornecerá as credenciais e as permissões necessárias para acessar os recursos atribuídos. À medida que você usa mais atributos do Nimble Studio para fazer seu trabalho, você pode precisar de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um atributo no Nimble Studio, consulte Solução de problemas de identidade e acesso do Amazon Nimble Studio.

Administrador de serviço – Se você é responsável pelos recursos do Nimble Studio em sua empresa, provavelmente tem acesso total ao Nimble Studio. É sua função determinar quais recursos e atributos do Nimble Studio seus funcionários devem acessar. Em seguida, envie solicitações ao administrador para alterar as permissões dos usuários do serviço. Revise as informações nesta página para entender os conceitos básicos doIAM. Para saber mais sobre como sua empresa pode usar o IAM Nimble Studio, consulteComo o Amazon Nimble Studio funciona com IAM.

Autenticando com identidades

Autenticação é como você faz login em AWS usando suas credenciais de identidade. Para obter mais informações sobre como fazer login usando o AWS Management Console, consulte Fazer login no AWS Management Console como IAM usuário ou usuário root no Guia do IAM usuário.

Você precisa estar autenticado (conectado em AWS) como o Conta da AWS usuário root, um usuário ou assumindo uma IAM função. Também é possível usar a autenticação de logon único da sua empresa ou até mesmo fazer login usando o Google ou Facebook. Nesses casos, seu administrador configurou anteriormente a federação de identidades usando IAM funções. Quando você acessa AWS usando credenciais de outra empresa, você está assumindo uma função indiretamente.

Para fazer login diretamente no AWS Management Console, use sua senha com o endereço de e-mail do usuário root ou seu nome de usuário. Você pode acessar AWS usando programaticamente o usuário root ou as chaves de acesso do usuário.

AWS fornece ferramentas SDK de linha de comando para assinar criptograficamente sua solicitação usando suas credenciais. Se você não usa AWS ferramentas, assine a solicitação você mesmo. Faça isso usando o Signature Version 4, um protocolo para autenticar solicitações de entradaAPI. Para obter mais informações sobre solicitações de autenticação, consulte Processo de assinatura do Signature versão 4 no Referência geral da AWS .

Independentemente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Como usar a autenticação multifator (MFA) em AWSno Guia do IAM usuário.

Conta da AWS usuário raiz

Quando você cria pela primeira vez um Conta da AWS, você começa com uma identidade de login único que tem acesso completo a todos Serviços da AWS e recursos na conta. Essa identidade é chamada de Conta da AWS usuário root e é acessado fazendo login com o endereço de e-mail

e a senha que você usou para criar a conta. Recomendamos fortemente que você não utilize o usuário-raiz para suas tarefas diárias, mesmo as administrativas. Em vez disso, siga a prática recomendada de usar o usuário root somente para criar seu primeiro IAM usuário. Depois, guarde as credenciais do usuário raiz em um lugar seguro e utilize-as para executar somente algumas tarefas de gerenciamento de contas e serviços.

Usuários e grupos

Um usuário é uma identidade dentro do seu Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Um usuário pode ter credenciais de longo prazo ou um conjunto de chaves de acesso. Para saber como gerar chaves de acesso, consulte Gerenciamento de chaves de acesso para IAM usuários no Guia IAM do usuário. Ao gerar chaves de acesso para um usuário, visualize e salve com segurança o par de chaves. Você não poderá recuperar a chave de acesso secreta no futuro. Em vez disso, gere um novo par de chaves de acesso.

Um IAMgrupo é uma identidade que especifica uma coleção de usuários. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um grupo chamado IAMAdminse conceder a esse grupo permissões para administrar IAM recursos.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a uma aplicação, mas um perfil pode ser assumido por qualquer pessoa que precisar dele. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias. Para saber mais, consulte Quando criar um usuário (em vez de uma função) no Guia do IAM usuário.

IAMfunções

Um IAMpapel é uma identidade dentro de você Conta da AWS que tem permissões específicas. É semelhante a um usuário, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma IAM função no AWS Management Console trocando de papéis. Você pode assumir uma função chamando um AWS CLI ou AWS APIoperação ou usando um personalizadoURL. Para obter mais informações sobre métodos de uso de funções, consulte Usando IAM funções no Guia IAM do usuário.

IAMfunções com credenciais temporárias são úteis nas seguintes situações:

- Permissões temporárias de usuário — Um usuário pode assumir uma IAM função para assumir temporariamente diferentes permissões para uma tarefa específica.

- Acesso de usuário federado — Em vez de criar um usuário, você pode usar identidades existentes de AWS Directory Service, seu diretório de usuários corporativos ou um provedor de identidade na web. Estes são conhecidos como usuários federados. AWS atribui uma função a um usuário federado quando o acesso é solicitado por meio de um provedor de identidade. Para obter mais informações sobre usuários federados, consulte Usuários e funções federados no Guia do IAM usuário.
  - Associação – O Nimble Studio usa um conceito chamado “associação” para fornecer ao usuário acesso a um perfil de execução específico. A associação permite que os administradores do estúdio deleguem acesso aos recursos aos usuários, sem precisar escrever ou entender políticas. IAM Quando um administrador do Nimble Studio cria uma associação para um usuário em um perfil de lançamento, o usuário está autorizado a realizar IAM ações necessárias para usar um perfil de lançamento, como visualizar suas propriedades e iniciar uma sessão de streaming usando esse perfil de lançamento.
  - Função de serviço — Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Os perfis de serviço fornecem acesso somente na sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Um administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS service (Serviço da AWS)no Guia do IAM usuário.
  - Função vinculada a serviços — Uma função vinculada a serviços é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de realizar uma ação em seu nome. O Nimble Studio não oferece suporte às funções vinculadas ao serviço.
- Aplicativos em execução na Amazon EC2 — Você pode usar uma IAM função para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma EC2 instância e fazendo AWS CLI ou AWS APIsolicitações. Isso é preferível a armazenar chaves de acesso na EC2 instância. Para atribuir um AWS Ao atribuir a uma EC2 instância e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância que é anexado à instância. Um perfil de instância contém a função e permite que programas em execução na EC2 instância recebam credenciais temporárias. Para obter mais informações, consulte Como usar uma IAM função para conceder permissões a aplicativos executados em EC2 instâncias da Amazon no Guia IAM do usuário.

Para saber se usar IAM funções ou usuários, consulte Quando criar uma IAM função (em vez de um usuário) no Guia do IAM usuário.

Gerenciando acesso usando políticas

Você controla o acesso em AWS criando políticas e anexando-as a IAM identidades ou AWS recursos. Uma política é um objeto em AWS que, quando associados a uma identidade ou recurso, definem suas permissões. Você pode entrar como usuário raiz ou usuário, ou pode assumir uma IAM função. Quando você faz uma solicitação, AWS avalia as políticas relacionadas baseadas em identidade ou recursos. As permissões nas políticas determinam se a solicitação será permitida ou negada. A maioria das políticas é armazenada em AWS como JSON documentos. Para obter mais informações sobre a estrutura e o conteúdo dos documentos de JSON política, consulte Visão geral das JSON políticas no Guia IAM do usuário.

Os administradores podem usar AWS JSONpolíticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações sobre quais recursos e em quais condições.

Cada IAM entidade (usuário ou função) começa sem permissões. Em outras palavras, por padrão, os usuários não podem fazer nada, nem mesmo alterar sua própria senha. Para dar permissão a um usuário para fazer algo, um administrador deve anexar uma política de permissões ao usuário. Ou o administrador pode adicionar o usuário a um grupo que tenha as permissões pretendidas. Quando um administrador concede permissões a um grupo, todos os usuários desse grupo recebem essas permissões.

IAMas políticas definem permissões para uma ação, independentemente do método usado para realizar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações sobre a função do AWS Management Console, o AWS CLI, ou o AWS API.

Políticas baseadas em identidade

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um usuário, grupo de usuários ou função. Estas políticas controlam quais ações os usuários e funções podem executar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAM usuário.

As políticas baseadas em identidade podem ser categorizadas ainda adicionalmente como políticas em linha ou políticas gerenciadas. As políticas em linha são anexadas diretamente a um único usuário, grupo ou perfil. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas gerenciadas incluem AWS políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como escolher entre uma

política gerenciada ou uma política em linha, consulte Escolha entre políticas gerenciadas e políticas em linha no Guia do IAM usuário.

Políticas baseadas no recurso

Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em quais condições. Especifique uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Políticas baseadas em recursos são políticas em linha localizadas nesse serviço. Você não pode usar AWS políticas gerenciadas a partir IAM de uma política baseada em recursos.

Listas de controle de acesso (ACLs) no Nimble Studio

As listas de controle de acesso (ACLs) controlam quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato do documento JSON de política.

Amazon S3, AWS WAF, e a Amazon VPC são exemplos de serviços que oferecem suporteACLs. Para saber maisACLs, consulte a visão geral da lista de controle de acesso (ACL) no Guia do desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões — Um limite de permissões é um recurso avançado no qual você define as permissões máximas que uma política baseada em identidade pode conceder a uma IAM entidade (usuário ou função). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a intersecção das políticas baseadas em identidade da entidade e dos seus limites de permissões. As políticas baseadas em recursos que especificam o usuário ou a função no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações

sobre limites de permissões, consulte Limites de permissões para IAM entidades no Guia IAM do usuário.

- Políticas de controle de serviço (SCPs) — SCPs são JSON políticas que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em Organizations. Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os recursos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as suas contas. Os SCP limites de permissões para entidades em contas de membros, incluindo cada Conta da AWS usuário root. Para obter mais informações sobre Organizations eSCPs, consulte Como SCPs trabalhar no AWS Organizations Guia do usuário.
- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para um perfil ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou da função e as políticas da sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia IAM do usuário.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determina se uma solicitação deve ser permitida quando vários tipos de política estão envolvidos, consulte Lógica de avaliação de políticas no Guia IAM do usuário.

Como o Amazon Nimble Studio funciona com IAM

Antes de usar IAM para gerenciar o acesso ao Nimble Studio, saiba quais IAM recursos estão disponíveis para uso com o Nimble Studio.

IAMrecursos que você pode usar com o Amazon Nimble Studio

IAMrecurso	Suporte do Nimble Studio
Ações de políticas do Nimble Studio	Sim
Recursos de políticas para o Nimble Studio	Sim

IAMrecurso	Suporte do Nimble Studio
Chaves de condição de política para Nimble Studio	Sim
Listas de controle de acesso (ACLs) no Nimble Studio	Não
Controle de acesso baseado em atributos (ABAC) com o Nimble Studio	Sim
Usando credenciais temporárias com Nimble Studio	Sim
Permissões de entidades principais entre serviços para o Nimble Studio	Sim
Perfis de serviço do Nimble Studio	Sim
Funções vinculadas ao serviço para o Nimble Studio	Não

Para obter uma visão de alto nível de como o Nimble Studio e outros Serviços da AWS funciona com a maioria dos IAM recursos, consulte Serviços da AWS que funcionam com IAM o Guia IAM do Usuário.

Políticas do Nimble Studio baseadas em identidade

Suporta políticas baseadas em identidade	Sim

Políticas baseadas em identidade são documentos de políticas de JSON permissões que você pode anexar a uma identidade, como um usuário, grupo de usuários ou função. Estas políticas controlam quais ações os usuários e funções podem executar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte Criação de IAM políticas no Guia do IAM usuário.

Com políticas IAM baseadas em identidade, você pode especificar ações e recursos permitidos ou negados, bem como as condições para as quais as ações são permitidas ou negadas. Não é

possível especificar a entidade principal de segurança em uma política baseada em identidade porque ela se aplica ao usuário ou à função à qual está anexada. Para saber mais sobre todos os elementos que você pode usar em uma JSON política, consulte a referência IAM JSON de elementos de política no Guia IAM do usuário.

Exemplos de políticas baseadas em identidade para Amazon Nimble Studio

Para visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

Políticas baseadas em recursos no Nimble Studio

Oferece compatibilidade com políticas baseadas em recursos	Não

O Nimble Studio não oferece suporte a políticas baseadas em recursos ou acesso entre contas. Políticas baseadas em recursos são documentos JSON de política que você anexa a um recurso. Exemplos de políticas baseadas em recursos são políticas de confiança de IAM funções e políticas de bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal especificada pode executar nesse recurso e em quais condições. Especifique uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou Serviços da AWS.

Ações de políticas do Nimble Studio

Oferece compatibilidade com ações de políticas	Sim

Os administradores podem usar AWS JSONpolíticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações sobre quais recursos e em quais condições.

O `Action` elemento de uma JSON política descreve as ações que você pode usar para permitir ou negar acesso em uma política. As ações de política geralmente têm o mesmo nome que as associadas AWS APIoperação. Há algumas exceções, como ações somente com permissão que não

têm uma operação correspondente. API Algumas operações também exigem várias ações em uma política. Essas ações adicionais são chamadas de ações dependentes.

Incluem ações em uma política para conceder permissões para executar a operação associada.

Para ver uma lista de ações do Nimble Studio, consulte Ações definidas pelo Amazon Nimble Studio na Referência de autorização de serviço.

As ações de política no Nimble Studio usam o seguinte prefixo antes da ação:

```
nimble
```

Para especificar várias ações em uma única instrução, separe-as com vírgulas.

```
"Action": [
      "nimble:action1",
      "nimble:action2"
         ]
```

Para visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

Recursos de políticas para o Nimble Studio

Oferece compatibilidade com recursos de políticas	Sim

Os administradores podem usar AWS JSONpolíticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações sobre quais recursos e em quais condições.

O elemento `Resource` JSON de política especifica o objeto ou objetos aos quais a ação se aplica. As instruções devem incluir um elemento `Resource` ou `NotResource`. Como prática recomendada, especifique um recurso usando seu Amazon Resource Name (ARN). Isso pode ser feito para ações que oferecem compatibilidade com um tipo de recurso específico, conhecido como permissões em nível de recurso.

Para ações que não oferecem suporte a permissões em nível de recurso, como operações de listagem, use um curinga (*) para indicar que a instrução se aplica a todos os recursos.

```
"Resource": "*"
```

Para visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

Chaves de condição de política para Nimble Studio

Oferece suporte a chaves de condição de políticas	Sim

Os administradores podem usar AWS JSONpolíticas para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações sobre quais recursos e em quais condições.

O elemento `Condition` (ou elemento `Condition`**`block`**`) lets you specify conditions in which a statement is in effect. The `Condition`) é opcional. É possível criar expressões condicionais que usem agentes de condição, como “igual a” ou “menor que”, para fazer a condição da política corresponder aos valores na solicitação.

Se você especificar vários `Condition` elementos em uma instrução ou várias chaves em um único `Condition` elemento, AWS os avalia usando uma `AND` operação lógica. Se você especificar vários valores para uma única chave de condição, AWS avalia a condição usando uma `OR` operação lógica. Todas as condições devem ser atendidas para que as permissões da instrução sejam concedidas.

Você também pode usar variáveis de espaço reservado ao especificar condições. Por exemplo, você pode conceder permissão a um usuário para acessar um recurso somente se ele estiver marcado com seu nome de usuário. Para obter mais informações, consulte elementos de IAM política: variáveis e tags no Guia IAM do usuário.

AWS suporta chaves de condição globais e chaves de condição específicas do serviço. Para ver tudo AWS chaves de condição globais, consulte AWS chaves de contexto de condição global no Guia IAM do usuário.

Para visualizar exemplos de políticas baseadas em identidade do Nimble Studio, consulte Exemplos de políticas baseadas em identidade para Amazon Nimble Studio.

Listas de controle de acesso (ACLs) no Nimble Studio

Suporta ACLs	Não

O Nimble Studio não oferece suporte a listas de controle de acesso (ACLs). ACLscontrolar quais diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLssão semelhantes às políticas baseadas em recursos, embora não usem o formato do documento JSON de política.

Controle de acesso baseado em atributos (ABAC) com o Nimble Studio

Suportes ABAC (tags nas políticas)	Sim

O controle de acesso baseado em atributos (ABAC) é uma estratégia de autorização que define permissões com base em atributos. Em AWS, esses atributos são chamados de tags. Você pode anexar tags a IAM entidades (usuários ou funções) e a muitas AWS recursos. Marcar entidades e recursos é a primeira etapa doABAC. Em seguida, você cria ABAC políticas para permitir operações quando a tag do diretor corresponde à tag do recurso que ele está tentando acessar.

Para controlar o acesso baseado em tags, forneça informações sobre as tags no elemento de condição de uma política usando as `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou chaves de condição `aws:TagKeys`.

Para obter mais informações sobreABAC, consulte O que éABAC? no Guia do IAM usuário. Para ver um tutorial com etapas de configuraçãoABAC, consulte Usar controle de acesso baseado em atributos (ABAC) no Guia do IAM usuário.

Usando credenciais temporárias com Nimble Studio

Oferece compatibilidade com credenciais temporárias	Sim

Alguns Serviços da AWS não funcionam quando você faz login usando credenciais temporárias. Para obter informações adicionais, incluindo quais Serviços da AWS trabalhar com credenciais temporárias, consulte Serviços da AWS que funcionam com IAM o Guia IAM do Usuário.

Você está usando credenciais temporárias se fizer login no AWS Management Console usando qualquer método, exceto um nome de usuário e senha. Por exemplo, quando você acessa AWS usando o link de login único (SSO) da sua empresa, esse processo cria automaticamente credenciais temporárias. Você também cria automaticamente credenciais temporárias quando faz login no

console como usuário e, em seguida, alterna perfis. Para obter mais informações sobre a troca de funções, consulte Alternando para uma função (console) no Guia IAM do usuário.

Você pode criar manualmente credenciais temporárias usando o AWS CLI ou AWS API. Você pode então usar essas credenciais temporárias para acessar AWS. AWS recomenda que você gere credenciais temporárias dinamicamente em vez de usar chaves de acesso de longo prazo. Para obter mais informações, consulte Credenciais de segurança temporárias emIAM.

Permissões de entidades principais entre serviços para o Nimble Studio

Suporta permissões de entidades principais	Sim

Perfis de serviço do Nimble Studio

Oferece compatibilidade com funções de serviço	Sim

Uma função de serviço é uma IAMfunção que um serviço assume para realizar ações em seu nome. Os perfis de serviço fornecem acesso somente na sua conta e não podem ser usadas para conceder acesso a serviços em outras contas. Um administrador pode criar, modificar e excluir uma função de serviço internamenteIAM. Para obter mais informações, consulte Criação de uma função para delegar permissões a um AWS service (Serviço da AWS)no Guia do IAM usuário.

> **Warning**
>
> Alterar as permissões de um perfil de serviço pode interromper a funcionalidade do Nimble Studio. Edite perfis de serviço somente quando o Nimble Studio fornecer orientação para isso.

Funções vinculadas ao serviço para o Nimble Studio

Oferece suporte a perfis vinculados ao serviço	Não

O Nimble Studio não oferece suporte às funções vinculadas ao serviço. Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um AWS service (Serviço da AWS). O serviço pode assumir a função de realizar uma ação em seu nome. As funções vinculadas ao serviço aparecem em sua IAM conta e são de propriedade do serviço. Um administrador do pode visualizar, mas não pode editar as permissões para funções vinculadas ao serviço.

Para obter detalhes sobre como criar ou gerenciar funções vinculadas a serviços, consulte Serviços da AWS que funcionam com IAM. Encontre um serviço na tabela que inclua um `Yes` na coluna Função vinculada ao serviço. Escolha o link Sim para visualizar a documentação do perfil vinculado a serviço desse serviço.

Exemplos de políticas baseadas em identidade para Amazon Nimble Studio

Por padrão, usuários e funções não têm permissão para criar ou modificar recursos do Nimble Studio. Eles também não podem realizar tarefas usando o AWS Management Console, AWS CLI, ou AWS API. Um administrador deve criar IAM políticas que concedam aos usuários e funções permissão para realizar ações nos recursos de que precisam. O administrador deve anexar essas políticas aos usuários ou grupos que exigem essas permissões.

Para saber como criar uma política IAM baseada em identidade usando esses exemplos de documentos JSON de política, consulte Criação de políticas na JSON guia do IAM usuário.

Tópicos

- Melhores práticas de política

Melhores práticas de política

As políticas baseadas em identidade são muito eficientes. Eles determinam se alguém pode criar, acessar ou excluir recursos do Nimble Studio em sua conta. Essas ações podem incorrer em custos para o seu Conta da AWS. Ao criar ou editar políticas baseadas em identidade, siga estas diretrizes e recomendações:

- Comece a usar AWS políticas gerenciadas — Para começar a usar o Nimble Studio rapidamente, use AWS políticas gerenciadas para dar aos seus funcionários as permissões de que precisam. Essas políticas já estão disponíveis em sua conta e são mantidas e atualizadas por AWS. Para obter mais informações, consulte Começar a usar permissões com AWS políticas gerenciadas no Guia IAM do usuário.

- Conceder privilégio mínimo: ao criar políticas personalizadas, conceda apenas as permissões necessárias para executar uma tarefa. Comece com um conjunto mínimo de permissões e conceda permissões adicionais conforme necessário. Fazer isso é mais seguro do que começar com permissões que são muito lenientes e tentar restringi-las superiormente. Para obter mais informações, consulte Conceder privilégios mínimos no Guia do IAM usuário.
- Habilite MFA operações confidenciais — Para maior segurança, exija que os usuários usem a autenticação multifator (MFA) para acessar recursos ou API operações confidenciais. Para obter mais informações, consulte Usando a autenticação multifator (MFA) em AWSno Guia do IAM usuário.
- Utilize condições de política para segurança extra: Na medida em que for prático, defina as condições em que as suas políticas baseadas em identidade permitem o acesso a um recurso. Por exemplo, você pode gravar condições para especificar um intervalo de endereços IP permitidos do qual a solicitação deve partir. Você também pode criar condições para permitir solicitações somente dentro de um intervalo de data ou hora especificado, ou para exigir o uso de SSL ouMFA. Para obter mais informações, consulte elementos IAM JSON da política: Condição no Guia IAM do usuário.

AWS políticas gerenciadas para o Amazon Nimble Studio

Para adicionar permissões a usuários, grupos e funções, é mais fácil de usar AWS políticas gerenciadas do que escrever políticas você mesmo. É preciso tempo e experiência para criar políticas gerenciadas pelo IAM cliente que forneçam à sua equipe somente as permissões necessárias. Para começar rapidamente, você pode usar nosso AWS políticas gerenciadas. Essas políticas abrangem casos de uso comuns e estão disponíveis em Conta da AWS. Para obter mais informações sobre AWS políticas gerenciadas, consulte AWS políticas gerenciadas no Guia IAM do usuário.

AWS manutenção e atualização de serviços AWS políticas gerenciadas. Você não pode alterar as permissões no AWS políticas gerenciadas. Ocasionalmente, os serviços adicionam permissões adicionais a um AWS política gerenciada para oferecer suporte a novos recursos. Esse tipo de atualização afeta todas as identidades (usuários, grupos e funções) em que a política está anexada. É mais provável que os serviços atualizem um AWS política gerenciada quando um novo recurso é lançado ou quando novas operações são disponibilizadas. Os serviços não removem permissões de um AWS política gerenciada, para que as atualizações de políticas não violem suas permissões existentes.

Além disso, AWS oferece suporte a políticas gerenciadas para funções de trabalho que abrangem vários serviços. Por exemplo, o ReadOnlyAccess AWS a política gerenciada fornece acesso somente de leitura a todos AWS serviços e recursos. Quando um serviço lança um novo recurso, AWS adiciona permissões somente de leitura para novas operações e recursos. Para obter uma lista e descrições das políticas de funções de trabalho, consulte AWS políticas gerenciadas para funções de trabalho no Guia IAM do usuário.

Seus usuários finais acessarão o Amazon Nimble Studio principalmente usando o portal do Nimble Studio. Ao criar seu estúdio usando StudioBuilder o console do Nimble Studio, uma IAM função é criada para cada personagem do estúdio: o administrador do estúdio e o usuário do estúdio. Cada um tem a respectiva política IAM gerenciada anexada. O portal do Nimble Studio fornece uma experiência em que os usuários só podem listar e usar os recursos que eles têm permissão para acessar.

O portal do Nimble Studio fornece uma experiência em que os usuários só podem listar e usar os recursos aos quais têm acesso, e o portal depende do conteúdo dessas políticas para operar corretamente. Os usuários finais do Nimble Studio usarão o portal para acessar seu estúdio na nuvem. Então, quando os administradores criam seu estúdio usando StudioBuilder, uma IAM função é criada para cada pessoa que precisa acessar o estúdio. Isso inclui o administrador e o usuário do estúdio, cada um com sua respectiva política IAM gerenciada anexada.

Para obter uma lista e descrições das políticas de funções de trabalho, consulte AWS políticas gerenciadas para funções de trabalho no Guia IAM do usuário.

AWS política gerenciada: `AmazonNimbleStudio-LaunchProfileWorker`

Você pode anexar a `AmazonNimbleStudio-LaunchProfileWorker`política às suas IAM identidades.

Anexe essa política às EC2 instâncias criadas pelo Nimble Studio Builder para conceder acesso aos recursos necessários aos trabalhadores do perfil de lançamento do Nimble Studio.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- ds - Permite que LaunchProfile os trabalhadores descubram informações de conexão sobre o AWS Managed Microsoft AD associado a um LaunchProfile.
- ec2 - Permite que LaunchProfile os trabalhadores descubram informações de grupos de segurança e sub-redes para se conectar a um. LaunchProfile

- fsx - Permite que LaunchProfile os trabalhadores descubram informações de conexão com FSx volumes da Amazon associados a um LaunchProfile.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      },
      "Sid": "GetLaunchProfileInitializationDependencies"
    }
  ],
  "Version": "2012-10-17"
}
```

AWS política gerenciada: **AmazonNimbleStudio-StudioAdmin**

Você pode anexar a AmazonNimbleStudio-StudioAdminpolítica às suas IAM identidades.

Anexe essa política à função de administrador associada ao seu estúdio para conceder acesso aos recursos do Amazon Nimble Studio associados ao administrador do estúdio e aos recursos relacionados do estúdio em outros serviços.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- nimble - Permite que os usuários do Studio acessem os recursos do Nimble que foram delegados a eles por. StudioAdmins

- sso - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.
- identitystore - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.
- ds - Permite que o Nimble Studio adicione estações de trabalho virtuais ao AWS Managed Microsoft AD associado ao estúdio.
- ec2 - Permite que o Nimble Studio conecte estações de trabalho virtuais à sua configuração. VPC
- fsx - Permite que o Nimble Studio conecte estações de trabalho virtuais aos seus volumes Amazon configurados. FSx
- cloudwatch - Permite que o Nimble Studio recupere métricas. CloudWatch

```
{
  "Statement": [
    {
      "Sid": "StudioAdminFullAccess",
      "Effect": "Allow",
      "Action": [
        "nimble:CreateStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:DeleteStreamingSession",
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetEula",
        "nimble:AcceptEulas",
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListStreamingSessions",
        "nimble:GetStreamingImage",
        "nimble:ListStreamingImages",
        "nimble:GetLaunchProfileInitialization",
        "nimble:GetLaunchProfileDetails",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents",
        "nimble:ListLaunchProfiles",
        "nimble:GetLaunchProfile",
```

```
        "nimble:GetLaunchProfileMember",
        "nimble:ListLaunchProfileMembers",
        "nimble:PutLaunchProfileMembers",
        "nimble:UpdateLaunchProfileMember",
        "nimble:DeleteLaunchProfileMember"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ds:DescribeDirectories",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
```

```
      "Effect": "Allow",
      "Action": "cloudwatch:GetMetricData",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "cloudwatch:namespace": "AWS/NimbleStudio"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

AWS política gerenciada: **AmazonNimbleStudio-StudioUser**

Você pode anexar a AmazonNimbleStudio-StudioUserpolítica às suas IAM identidades.

Anexe esta política à função de usuário associada ao seu estúdio para conceder acesso aos recursos do Amazon Nimble Studio associados ao usuário do estúdio e aos recursos de estúdio relacionados em outros serviços.

Detalhes das permissões

Esta política inclui as seguintes permissões:

- nimble - Permite que os usuários do Studio acessem os recursos do Nimble que foram delegados a eles por. StudioAdmins
- sso - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.
- identitystore - Permite que os usuários do Studio visualizem os nomes de outros usuários no estúdio.
- ds - Permite que o Nimble Studio adicione estações de trabalho virtuais ao AWS Managed Microsoft AD associado ao estúdio.
- ec2 - Permite que o Nimble Studio conecte estações de trabalho virtuais à sua configuração. VPC
- fsx - Permite que o Nimble Studio conecte estações de trabalho virtuais aos seus volumes Amazon configurados. FSx

```
{
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
        "ds:CreateComputer",
        "ec2:DescribeSubnets",
        "ec2:CreateNetworkInterfacePermission",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterfacePermission",
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeSecurityGroups",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "nimble.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:DescribeUsers",
        "sso-directory:SearchUsers",
        "identitystore:DescribeUser",
        "identitystore:ListUsers"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListLaunchProfiles"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:requesterPrincipalId": "${nimble:principalId}"
        }
```

```
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:ListStudioMembers",
        "nimble:GetStudioMember",
        "nimble:ListEulas",
        "nimble:ListEulaAcceptances",
        "nimble:GetFeatureMap",
        "nimble:PutStudioLogEvents"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "nimble:StartStreamingSession",
        "nimble:StopStreamingSession",
        "nimble:DeleteStreamingSession",
        "nimble:GetStreamingSession",
        "nimble:CreateStreamingSessionStream",
        "nimble:GetStreamingSessionStream",
        "nimble:ListStreamingSessions"
        "nimble:ListStreamingSessionBackups",
        "nimble:GetStreamingSessionBackup"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "nimble:ownedBy": "${nimble:requesterPrincipalId}"
        }
      }
    }
  ],
  "Version": "2012-10-17"
}
```

Atualizações do Nimble Studio para AWS políticas gerenciadas

Exibir detalhes sobre as atualizações do AWS gerenciei políticas para o Amazon Nimble Studio desde que esse serviço começou a rastrear essas mudanças.

Alteração	Descrição	Data
AWS política gerenciada: AmazonNimbleStudio-StudioUser: Atualizar política	O Amazon Nimble Studio atualizou uma política para usar a versão mais recente do serviço Identity Store.	22 de setembro de 2023
AWS política gerenciada: AmazonNimbleStudio-StudioAdmin: Atualizar política	O Amazon Nimble Studio atualizou uma política para usar a versão mais recente do serviço Identity Store.	22 de setembro de 2023
AWS política gerenciada: AmazonNimbleStudio-StudioUser: Atualizar política	O Amazon Nimble Studio atualizou uma política para permitir que os usuários do estúdio visualizem seus backups de estações de trabalho.	20 de dezembro de 2022
AWS política gerenciada: AmazonNimbleStudio-StudioAdmin: Atualizar política	O Amazon Nimble Studio atualizou a política para permitir que os administr adores do estúdio visualizem seus backups de estações de trabalho.	20 de dezembro de 2022
AWS política gerenciada: AmazonNimbleStudio-StudioUser: Atualizar política	O Amazon Nimble Studio atualizou uma política para permitir que os administr adores do estúdio recuperem métricas. CloudWatch	11 de novembro de 2021
AWS política gerenciada: AmazonNimbleStudio-StudioUser: Atualizar política	O Amazon Nimble Studio atualizou a política para permitir que os usuários do estúdio iniciem e parem suas estações de trabalho.	1º de novembro de 2023

Alteração	Descrição	Data
AWS política gerenciada: `AmazonNimbleStudio-StudioAdmin` : Atualizar política	O Amazon Nimble Studio atualizou a política para permitir que os administradores do estúdio iniciem e parem suas estações de trabalho.	1º de novembro de 2023
AWS política gerenciada: `AmazonNimbleStudio-StudioUser` : Atualizar política	O Amazon Nimble Studio atualizou a política para permitir condicionalmente o acesso aos recursos da sessão de streaming com base em `nimble:ownedBy` em vez de `nimble:createdBy` .	16 de agosto de 2021
AWS política gerenciada: `AmazonNimbleStudio-StudioUser` – Nova política	O Amazon Nimble Studio adicionou uma nova política que permite o acesso aos recursos associados ao usuário do estúdio e aos recursos relacionados do estúdio em outros serviços.	28 de abril de 2021
AWS política gerenciada: `AmazonNimbleStudio-StudioAdmin` : nova política	O Amazon Nimble Studio adicionou uma nova política que permite o acesso aos recursos associados ao administrador do estúdio e aos recursos relacionados do estúdio em outros serviços.	28 de abril de 2021

Alteração	Descrição	Data
AWS política gerenciada: `AmazonNimbleStudio-LaunchProfileWorker` – Nova política	O Amazon Nimble Studio adicionou uma nova política que permite o acesso aos recursos necessários aos operadores do perfil de execução do Nimble Studio.	28 de abril de 2021
O Amazon Nimble Studio começou a monitorar alterações	O Amazon Nimble Studio começou a monitorar as mudanças em seu AWS políticas gerenciadas.	28 de abril de 2021

Prevenção do problema do substituto confuso entre serviços

O problema do substituto confuso é um problema de segurança em que uma entidade que não tem permissão para executar uma ação pode coagir uma entidade mais privilegiada a executar a ação. Em AWS, a falsificação de identidade entre serviços pode resultar no problema confuso do deputado. A personificação entre serviços pode ocorrer quando um serviço (o serviço de chamada) chama outro serviço (o serviço chamado). O serviço de chamada pode ser manipulado para que ele use as respectivas permissões com o objetivo de acessar os recursos de outro cliente de uma forma que, normalmente, ele não deveria ter permissão. Para evitar isso, AWS fornece ferramentas que ajudam você a proteger seus dados para todos os serviços com diretores de serviços que receberam acesso aos recursos em sua conta.

Recomendamos usar as chaves de contexto de condição `aws:SourceAccount` global `aws:SourceArn` e as chaves de contexto nas políticas de recursos para limitar as permissões que o Identity and Access Management (IAM) concede ao Amazon Nimble Studio para acessar seus recursos. Se você utilizar ambas as chaves de contexto de condição global, o valor `aws:SourceAccount` e a conta `aws:SourceArn` no valor deverão utilizar o mesmo ID de conta quando utilizados na mesma instrução de política.

O valor de `aws:SourceArn` deve ser do estúdio ARN e `aws:SourceAccount` deve ser o ID da sua conta. Você não saberá qual é o ID do estúdio até que o estúdio seja criado, pois ele é gerado pelo Nimble Studio. Depois que seu estúdio for criado, você poderá atualizar a política de confiança com o ID final do estúdio definido como `aws:SourceArn`.

A maneira mais eficaz de se proteger contra o confuso problema do deputado é usar a chave de contexto ARN de condição `aws:SourceArn` global com todo o recurso. Se você não souber a totalidade ARN do recurso ou se estiver especificando vários recursos, use a chave de condição de contexto `aws:SourceArn` global com curingas (*) para as partes desconhecidas do. ARN Por exemplo, `arn:aws:nimble::123456789012:*`.

Seus usuários finais assumem sua função de estúdio quando entram no portal do Nimble Studio. Quando você cria seu estúdio, AWS configura a função e avalia a política. AWS avalia a política toda vez que um de seus usuários fizer login no portal do Nimble Studio. Quando você cria um estúdio, não é possível modificar o `aws:SourceArn`. Depois de terminar de criar seu estúdio, você pode usar o seu studioArn para `aws:SourceArn` o.

O exemplo a seguir é uma política de assumir função que mostra como você pode usar as chaves de contexto de condição global `aws:SourceArn` e `aws:SourceAccount` no Nimble Studio para evitar o problema confused deputy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "identity.nimble.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:TagSession"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "123456789012"
        },
        "StringLike": {
          "aws:SourceArn": "arn:aws:nimble:us-west-2:123456789012:studio/*"
        }
      }
    }
  ]
}
```

Solução de problemas de identidade e acesso do Amazon Nimble Studio

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com o Nimble Studio e. IAM

Tópicos

Não estou autorizado a realizar uma ação no Nimble Studio.

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, é preciso atualizar suas políticas para permitir que você realize a ação.

O exemplo de erro a seguir ocorre quando o `mateojackson` IAM usuário tenta usar o console para ver detalhes sobre um *`my-example-widget`* recurso fictício, mas não tem as permissões fictícias`nimble:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 nimble:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `nimble:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam:PassRole.

Se você receber um erro informando que não está autorizado a executar a ação `iam:PassRole`, entre em contato com seu administrador para obter assistência. Peça que atualizem suas políticas para permitir que você passe uma função para o Nimble Studio.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço, em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazer isso, você precisa de permissões para passar a função ao serviço.

O erro de exemplo a seguir ocorre quando um usuário chamado `johndoe` tenta usar o console para executar uma ação no Nimble Studio. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. John não tem permissões para passar a função para o serviço.

```
User: arn:aws:iam::123456789012:user/johndoe is not authorized to perform: iam:PassRole
```

Nesse caso, John pede ao administrador para atualizar suas políticas e conceder permissão para executar a ação `iam:PassRole`.

Quero visualizar minhas chaves de acesso

O Amazon Nimble Studio não fornece chaves de acesso. Para saber mais sobre chaves de acesso secretas, consulte Gerenciamento de chaves de acesso no Guia IAM do usuário.

> **Important**
>
> Não forneça suas chaves de acesso a terceiros, mesmo para ajudar a encontrar seu ID de usuário canônico. Ao fazer isso, você pode dar a alguém acesso permanente à sua conta.

Ao criar um par de chaves de acesso, você será solicitado a salvar o ID da chave de acesso e a chave de acesso secreta em um local seguro. A chave de acesso secreta só está disponível no momento em que é criada. Se você perder sua chave de acesso secreta, adicione novas chaves de acesso ao seu usuário. Você pode ter no máximo duas chaves de acesso. Se você já possui dois, exclua um par de chaves antes de criar um novo. Para ver as instruções, consulte Gerenciamento de chaves de acesso no Guia IAM do usuário.

Sou administrador e quero permitir que outras pessoas acessem o Nimble Studio.

Para permitir que outras pessoas acessem o Nimble Studio, crie uma IAM entidade (usuário ou função) para a pessoa ou aplicativo que precisa de acesso. Eles usarão as credenciais dessa entidade para acessar AWS. Em seguida, anexe uma política à entidade que conceda as permissões corretas.

O Nimble Studio fornece a você `AmazonNimbleStudio-StudioUser` o AWS Management Console. O administrador de TI que gerencia o console usa essa política para conceder acesso ao estúdio a outras pessoas.

Para ver um tutorial sobre como usar a política administrativa, consulte o guia Configurar o Nimble Studio. Para saber como vincular políticas existentes aos usuários, como políticas de perfil de usuário e de lançamento, consulte Criação de IAM usuários (console).

Para obter informações sobre a importação de políticas, consulte Como criar seu primeiro usuário e grupo IAM delegados no Guia do IAMusuário.

Quero permitir que pessoas fora da minha Conta da AWS para acessar meus recursos do Nimble Studio.

Você pode criar um perfil que os usuários de outras contas ou pessoas fora da sua organização podem usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se o Nimble Studio oferece suporte a esses atributos, consulte Como o Amazon Nimble Studio funciona com IAM.
- Para saber como fornecer acesso aos seus recursos em Contas da AWS que você possui, consulte Fornecendo acesso a um IAM usuário em outro Conta da AWS que você possui no Guia do IAM Usuário.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Fornecendo acesso a Contas da AWS propriedade de terceiros no Guia do IAM Usuário.
- Para saber como fornecer acesso por meio da federação de identidades, consulte Fornecendo acesso a usuários autenticados externamente (federação de identidades) no Guia do IAM usuário.
- Para saber a diferença entre usar funções e políticas baseadas em recursos para acesso entre contas, consulte Como as IAM funções diferem das políticas baseadas em recursos no Guia do usuário. IAM

Registro e monitoramento de eventos de segurança com o Nimble Studio

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Amazon Nimble Studio e do seu AWS soluções. Colete dados de monitoramento de todas as partes do seu AWS solução para que você possa depurar mais facilmente uma falha de vários pontos, caso ocorra.

AWS e o Nimble Studio fornecem ferramentas para monitorar seus recursos e responder a possíveis incidentes, incluindo e Registrando chamadas do Nimble Studio usando AWS CloudTrail AWS CloudFormation Guia do usuário.

Para obter mais informações sobre como o Amazon Nimble Studio funciona com AWS CloudFormation, incluindo exemplos JSON e YAML modelos, consulte a referência de recursos e propriedades do Amazon Nimble Studio no AWS CloudFormation Guia do usuário. Para entender como usar CloudFormation modelos, consulte AWS CloudFormation conceitos.

Tópicos

- Registrando chamadas do Nimble Studio usando AWS CloudTrail

Registrando chamadas do Nimble Studio usando AWS CloudTrail

O Amazon Nimble Studio está integrado com AWS CloudTrail, um serviço que fornece um registro das ações realizadas por um usuário, uma função ou um AWS service (Serviço da AWS) no Nimble Studio. CloudTrail captura todas as API chamadas para o Nimble Studio como eventos. As chamadas capturadas incluem chamadas do console do Nimble Studio e chamadas de código para as operações do Amazon Nimble Studio.

Se você criar uma trilha, poderá habilitar a entrega contínua de CloudTrail eventos para um bucket do Amazon S3, incluindo eventos para o Nimble Studio. Se você não configurar uma trilha, ainda poderá ver os eventos mais recentes no CloudTrail console no Histórico de eventos. Usando as informações coletadas por CloudTrail, você pode determinar a solicitação que foi feita ao Nimble Studio, o endereço IP do qual a solicitação foi feita, quem fez a solicitação, quando ela foi feita e detalhes adicionais.

Leia sobre o Nimble Studio em CloudTrail

CloudTrail está habilitado em seu Conta da AWS quando você cria a conta. Quando a atividade ocorre no Nimble Studio, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em seu Conta da AWS. Para obter mais informações, consulte Visualização de eventos com histórico de CloudTrail eventos.

Para um registro contínuo dos eventos em seu Conta da AWS, incluindo eventos para o Nimble Studio, crie uma trilha. Uma trilha permite CloudTrail entregar arquivos de log para um bucket do Amazon S3. Por padrão, quando você cria uma trilha no console, a trilha se aplica a todos Regiões da AWS. A trilha registra eventos de todas as regiões do AWS particiona e entrega os arquivos de log para o bucket do Amazon S3 que você especificar. Além disso, você pode configurar outros Serviços da AWS para analisar e agir ainda mais com base nos dados do evento coletados nos CloudTrail registros.

Para obter mais informações, consulte as informações a seguir.

Visão geral da criação de uma trilha

CloudTrail serviços e integrações suportados

Configurando SNS notificações da Amazon para CloudTrail

Recebendo arquivos de CloudTrail log de várias regiões

Recebendo arquivos de CloudTrail log de várias contas

As ações do Nimble Studio são registradas CloudTrail e documentadas no Amazon Nimble Studio Reference. API Por exemplo, chamadas para o CreateStudio GetStudio e DeleteStudio as ações geram entradas nos arquivos de CloudTrail log.

Cada entrada de log ou evento contém informações sobre quem gerou a solicitação. As informações de identidade ajudam a determinar:

- Se a solicitação foi feita com root ou AWS Identity and Access Management (IAM) credenciais do usuário.
- Se a solicitação foi feita com credenciais de segurança temporárias de um perfil ou de um usuário federado.
- Se a solicitação foi feita por outro serviço.

Para obter mais informações, consulte o elemento Identidade CloudTrail do usuário.

Noções básicas sobre entradas do arquivo de log do Nimble Studio

Uma trilha é uma configuração que permite a entrega de eventos como arquivos de log para um bucket do Amazon S3 que você especificar. CloudTrail os arquivos de log contêm uma ou mais entradas de log. Um evento representa uma única solicitação de qualquer fonte, e inclui informações sobre a ação solicitada, data e hora da ação, parâmetros de solicitação e assim por diante. CloudTrail os arquivos de log não são um rastreamento de pilha ordenado das API chamadas públicas, portanto, eles não aparecem em nenhuma ordem específica.

Este JSON exemplo mostra três ações:

- ACTION_1: CreateStudio
- ACTION_2: GetStudio
- ACTION_3: DeleteStudio

```
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:25:49Z"
            }
        }
    },
```

```
    "eventTime": "2021-03-08T23:25:49Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "CreateStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "displayName": "Studio Name",
        "studioName": "EXAMPLE-studioName",
        "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User",
        "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin"
    },
    "responseElements": {},
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:44:25Z"
            }
        }
```

```
    },
    "eventTime": "2021-03-08T23:44:25Z",
    "eventSource": "nimble.amazonaws.com",
    "eventName": "GetStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": null,
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
},
{
    "eventVersion": "0",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "EXAMPLE-PrincipalID:EXAMPLE-Session",
        "arn": "arn:aws:sts::111122223333:assumed-role/EXAMPLE-UserName/EXAMPLE-
Session",
        "accountId": "111122223333",
        "accessKeyId": "EXAMPLE-accessKeyId",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "EXAMPLE-PrincipalID",
                "arn": "arn:aws:iam::111122223333:role/EXAMPLE-UserName",
                "accountId": "111122223333",
                "userName": "EXAMPLE-UserName"
            },
            "webIdFederationData": {},
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2021-03-08T23:45:14Z"
            }
        }
    },
    "eventTime": "2021-03-08T23:44:14Z",
```

```
    "eventSource": "nimble.amazonaws.com",
    "eventName": "DeleteStudio",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "EXAMPLE-userAgent",
    "requestParameters": {
        "studioId": "us-west-2-EXAMPLE-studioId"
    },
    "responseElements": {
        "studio": {
            "adminRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-Admin",
            "displayName": "My New Studio Name",
            "homeRegion": "us-west-2",
            "ssoClientId": "EXAMPLE-ssoClientId",
            "state": "DELETING",
            "statusCode": "DELETING_STUDIO",
            "statusMessage": "Deleting studio",
            "studioEncryptionConfiguration": {
                "keyType": "AWS_OWNED_CMK"
            },
            "studioId": "us-west-2-EXAMPLE-studioId",
            "studioName": "EXAMPLE-studioName",
            "studioUrl": "https://sso111122223333.us-
west-2.portal.nimble.amazonaws.com",
            "tags": {},
            "userRoleArn": "arn:aws:iam::111122223333:role/EXAMPLE-ServiceRole-User"
        }
    },
    "requestID": "EXAMPLE-requestID",
    "eventID": "EXAMPLE-eventID",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333"
}
```


No exemplo, você notará que os eventos mostram a região, o endereço IP e outros "requestParameters", como "" e userRoleArn "adminRoleArn", que ajudarão você a identificar o evento. Você pode ver a hora e a data em "creationDate“e a origem da solicitação, que está marcada como" eventSource “: “nimble.amazonaws.com”.

CloudTrail está habilitado em seu Conta da AWS quando você cria a conta. Quando a atividade ocorre em IAM ou AWS STS, essa atividade é registrada em um CloudTrail evento junto com outros AWS service (Serviço da AWS) eventos no Histórico de eventos. Você pode visualizar, pesquisar e baixar eventos recentes em seu Conta da AWS.

AWS CloudTrail captura todas as API chamadas para IAM e AWS Security Token Service (AWS STS) como eventos, incluindo chamadas do console e API chamadas. Para saber mais sobre como usar CloudTrail com IAM e AWS STS, consulte Registro IAM e AWS STS APIchamadas com AWS CloudTrail.

Para obter mais informações sobre CloudTrail, consulte AWS CloudTrail Guia do usuário.

Para obter informações sobre outros serviços de monitoramento que a Amazon oferece, consulte o Guia CloudWatch do usuário da Amazon.

Validação de conformidade do Amazon Nimble Studio

O Amazon Nimble Studio segue o modelo de responsabilidade compartilhada, e a conformidade é compartilhada entre AWS e nossos clientes.

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS no escopo do Programa de Conformidade e escolha o programa de conformidade no qual você está interessado. Para obter informações gerais, consulte AWS Programas de conformidade .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixando relatórios em AWS Artifact.

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinado pela confidencialidade de seus dados, pelos objetivos de conformidade da sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos em AWS focados em segurança e conformidade.
- Arquitetura para HIPAA segurança e conformidade na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar HIPAA aplicativos elegíveis.

> **Note**
>
> Nem todos Serviços da AWS são HIPAA elegíveis. Para obter mais informações, consulte a Referência de serviços HIPAA elegíveis.

- AWS Recursos de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeie a orientação para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliando recursos com regras no AWS Config Guia do desenvolvedor — O AWS Config O serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes do setor e os regulamentos.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança em AWS. O Security Hub usa controles de segurança para avaliar sua AWS recursos e para verificar sua conformidade com os padrões e as melhores práticas do setor de segurança. Para obter uma lista dos serviços e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças ao seu Contas da AWS, cargas de trabalho, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, por exemplo PCIDSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Segurança da infraestrutura no Amazon Nimble Studio

Como um serviço gerenciado, o Amazon Nimble Studio é protegido por AWS segurança de rede global. Para obter mais informações sobre AWS serviços de segurança e como AWS protege a infraestrutura, consulte AWS Segurança na nuvem. Para projetar seu AWS ambiente usando as

melhores práticas para segurança de infraestrutura, consulte Proteção de infraestrutura no pilar de segurança AWS Estrutura bem arquitetada.

Você usa AWS APIchamadas publicadas para acessar o Nimble Studio pela rede. Os clientes devem oferecer suporte para:

- Segurança da camada de transporte (TLS). Exigimos TLS 1,2 e recomendamos TLS 1,3.
- Suítes de criptografia com sigilo direto perfeito (), como (Ephemeral PFS Diffie-Hellman) ou DHE (Elliptic Curve Ephemeral Diffie-Hellman). ECDHE A maioria dos sistemas modernos, como Java 7 e versões posteriores, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando uma ID de chave de acesso e uma chave de acesso secreta associada a um IAM principal. Ou você pode usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Práticas recomendadas de segurança do Nimble Studio

O Amazon Nimble Studio oferece vários atributos de segurança a serem considerados ao desenvolver e implementar suas próprias políticas de segurança. As melhores práticas a seguir são diretrizes gerais e não representam uma solução completa de segurança. Como essas melhores práticas podem não ser adequadas ou suficientes para o seu ambiente, trate-as como considerações úteis em vez de prescrições.

Monitorar

O monitoramento é uma parte importante da manutenção da confiabilidade, disponibilidade e desempenho do Nimble Studio e de seu AWS soluções. Para obter mais informações sobre como monitorar e responder aos eventos, consulte Registro e monitoramento de eventos de segurança com o Nimble Studio.

Proteção de dados

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS credenciais e configure contas individuais com AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use a autenticação multifator (MFA) com cada conta.

- UseSSL/TLSpara se comunicar com AWS recursos. Recomendamos TLS 1.2 ou posterior.
- Configure API e registre as atividades do usuário com AWS CloudTrail.
- Use AWS soluções de criptografia, junto com todos os controles de segurança padrão dentro Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados pessoais armazenados no Amazon S3.
- Se você precisar de FIPS 140-2 módulos criptográficos validados ao acessar AWS por meio de uma interface de linha de comando ou umaAPI, use um FIPS endpoint. Para obter mais informações sobre os FIPS endpoints disponíveis, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que você nunca coloque informações de identificação confidenciais, como números de conta dos seus clientes, em campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o Amazon Nimble Studio ou outro Serviços da AWS usando o consoleAPI, AWS CLI, ou AWS SDKs. Todos os dados inseridos no Amazon Nimble Studio ou em outros serviços podem ser coletados para inclusão em logs de diagnóstico. Ao fornecer um URL para um servidor externo, não inclua informações de credenciais no URL para validar sua solicitação para esse servidor.

Permissões

Gerencie o acesso ao AWS recursos usando usuários, IAM funções e concedendo o mínimo de privilégios aos usuários. Estabeleça políticas e procedimentos de gerenciamento de credenciais para criar, distribuir, alternar e revogar AWS credenciais de acesso. Para obter mais informações, consulte as IAM melhores práticas no Guia IAM do usuário.

Suporte para o Nimble Studio

Esta seção fornece opções de suporte para o Nimble Studio, como obter ajuda ao implantar ou usar o serviço e suas aplicações relacionadas.

Índice

Fórum do Nimble Studio

Se você tiver dúvidas sobre o Nimble Studio, visite o fórum do Nimble Studio. Lá você pode obter respostas da comunidade e dos moderadores do fórum AWS sobre os atributos, problemas técnicos e ajuda para solução de problemas do Nimble Studio.

Suporte de aplicações

O Nimble Studio fornece documentação adicional para as seguintes aplicações.

AWSThinkboxDeadline

Para obter ajuda com seu parque de renderização ou para saber como Deadline funciona, consulte a documentação AWSThinkboxDeadline.

Nimble Studio File Transfer

Para saber como a transferência de arquivos funciona, consulte o Guia do usuário do Nimble Studio File Transfer.

AWS Support Center

O Centro AWS Support é um centro para criar e gerenciar seus casos de suporte. Ele fornece acesso a uma variedade de recursos, incluindo soluções técnicas e de cobrança, um centro de

conhecimento, vídeos do centro de conhecimento, documentação AWS, além de treinamento e certificação.

Planos do AWS Support

Os planos AWS Support ajudam você a otimizar o desempenho, permanecer seguro, evitar o tempo de inatividade e controlar os custos. Para obter mais informações sobre planos AWS Support, consulte Comparar planos AWS Support.

Para obter mais informações sobre como AWS pode ajudá-lo, acesse a página Fale conosco.

Histórico do documentos

- Versão da API: mais recente
- Última atualização na documentação: 22 de setembro de 2023.

A tabela a seguir descreve as mudanças importantes em cada versão do Guia do administrador do Nimble.

Alteração	Descrição	
Serviço e guia novos	Esta é a versão inicial do Amazon Nimble Studio e do Guia do Administrador do Amazon Nimble Studio.	19 de junho de 2023
Atualização da política gerenciada AWS	Atualizou as políticas `AmazonNimbleStudio-StudioUser` e `AmazonNimbleStudio-StudioAdmin` para usar a versão mais recente do serviço AWS IAM Identity Center.	22 de setembro de 2023

Glossário do AWS

Para obter a terminologia mais recente da AWS, consulte o glossário da AWS na Referência do Glossário da AWS.

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.